RANDOM NUMBER GENERATOR

BACKGROUND OF THE INVENTION

Field of the Invention

The present invention relates to a random number generator formed from oscillators at different frequencies.

Description of the Related Art

Fig. 1 very schematically shows in the form of blocks a conventional example of a random number generator.

Such a generator uses a first voltage-controlled oscillator (VCO) 1 in a relatively high frequency range (HF). The control of oscillator 1 originates either from an oscillator of lower frequency (MF) (not shown) or from electronic noise generally coming from the same integrated circuit. The output of oscillator 1 provides a triangular signal of variable frequency intended to form, possibly after shaping by a comparator 2, input signal D of a flip-flop 3, output Q of which provides a digital train forming a random number. The function of comparator 2 simply is to shape as square pulses the signal provided by oscillator 1. For this purpose, one of its inputs, for example, its non-inverting input, receives the output of oscillator 1 while its other output (for example, inverting) receives a reference voltage provided by a resistive dividing bridge R1, R2 to the junction point of which is connected a filtering capacitor C providing the reference voltage for comparator 2.

A second oscillator 4 (OSC), at a relatively low frequency (BF) with respect to the frequency of oscillator 1 provides a clock signal to input CLK of flip-flop 3. Frequency BF of oscillator 4 is predetermined.

At each edge (for example, rising) of the output signal of oscillator 4, flip-flop 3 takes into account the state present on its D input. Since this state is at

zero or at one according to the signal provided by oscillator 1, the output of flip-flop 3 takes an output state 0 or 1. Since the output signal of oscillator 1 has a frequency conditioned by noise, the succession of states 1 or 0 at the output of flip-flop 3 forms a sequence of random states.

For the circuit of Fig. 1 to operate in this manner, oscillators 1 and 4 must not be synchronized. Indeed, if they are, a repetitive sequence of bits necessarily appears at the output of flip-flop 3. This is in particular why the voltage-control input of oscillator 1 is driven by a signal of intermediary frequency (that is, ranging between frequency BF and the minimum frequency of oscillator 1) or by noise. This is also why the output of oscillator 1 preferentially generates a triangular signal rather than a sinusoid to guarantee the equiprobable character of the output frequencies of oscillator 1. The frequency of oscillator 1 varies within a predetermined fixed range according to the position of a voltage control on the intermediary frequency ramp.

A disadvantage of the circuit of Fig. 1 is that there however remains a risk of oscillator synchronization. Indeed, a noise at the frequency of oscillator 1 transfers onto the supply and thus pollutes oscillator 4. This noise synchronizes the two signals. Indeed, the triggerings are performed with respect to thresholds. Now, the presence of HF noise superposed to the lower frequency imposes that the threshold triggerings will occur with priority on this noise. This effectively amounts to synchronizing the signals.

An example of a random number generator such as illustrated in Fig. 1 is described in article "The Intel Random number generator" by Benjamin Jun and Paul Kocher, published on April 22, 1999, by Cryptography Research Inc.

BRIEF SUMMARY OF THE INVENTION

An embodiment of the present invention provides a novel random number generator which overcomes the disadvantages of known oscillator generators.

An embodiment of the present invention more specifically aims at solving the problems linked to a possible synchronization of the signals from the high-frequency and low-frequency input oscillators of the flip-flop.

One embodiment of the present invention provides a generator of random numbers by a flip-flop having a data input receiving a first signal at a first frequency comprised in a predetermined range and the instantaneous value of which is conditioned by an interfering signal, and having a clock input receiving a second signal at a second predetermined frequency, smaller than the first one, said second signal crossing a delay element giving it a delay greater than or equal to the maximum period of the first signal.

According to an embodiment of the present invention, said disturbing signal is provided by a third oscillator at an intermediary frequency between said first and second frequencies.

According to an embodiment of the present invention, the generator further comprises a comparator for shaping the signal provided by the first oscillator before arrival on the data input of the flip-flop.

According to an embodiment of the present invention, the first oscillator is a voltage-controlled oscillator having a control input receiving said disturbing signal.

According to an embodiment of the present invention, the second frequency is selected to have a ratio of at least 100 with the minimum frequency of the first signal.

According to an embodiment of the present invention, the frequency of the intermediary signal is selected to have a ratio ranging between 5 and 20 with the minimum frequency of the first signal.

The foregoing features of the present invention will be discussed in detail in the following non-limiting description of specific embodiments in connection with the accompanying drawings.

BRIEF DESCRIPTION OF THE SEVERAL VIEWS OF THE DRAWINGS

Fig. 1, previously described, schematically shows in the form of blocks a conventional example of a random number generator;

Fig. 2 shows an embodiment of a random number generator according to the present invention; and

Fig. 3 illustrates, in timing diagrams, the operation of the generator of Fig. 2.

DETAILED DESCRIPTION

Embodiments of a random number generator are described herein. In the following description, numerous specific details are given to provide a thorough understanding of embodiments of the invention. One skilled in the relevant art will recognize, however, that the invention can be practiced without one or more of the specific details, or with other methods, components, materials, etc. In other instances, well-known structures, materials, or operations are not shown or described in detail to avoid obscuring aspects of the invention.

Reference throughout this specification to "one embodiment" or "an embodiment" means that a particular feature, structure, or characteristic described in connection with the embodiment is included in at least one embodiment of the present invention. Thus, the appearances of the phrases "in one embodiment" or "in an embodiment" in various places throughout this specification are not necessarily all referring to the same embodiment. Furthermore, the particular features, structures, or characteristics may be combined in any suitable manner in one or more embodiments.

Same elements have been designated with same reference numerals in the different drawings. For clarity, only those elements that are necessary to the understanding of the present invention have been shown in the drawings and will be described hereafter. In particular, the details constitutive of

the voltage-controlled oscillator, of the comparator, and of the flip-flop have not been detailed and are no object of the present invention.

A feature of one embodiment of the present invention is to delay by a predetermined duration the signal provided by an oscillator at a relatively low frequency of control of a flip-flop providing the random number sequence. According to an embodiment of the present invention, this predetermined duration preferably corresponds to the maximum period of a relatively high frequency likely to be provided by a voltage-controlled oscillator, the output of which conditions the flip-flop data input.

Fig. 2 schematically shows in the form of blocks an embodiment of a random number generator according to the present invention.

As previously, this generator is based on a flip-flop 3, the D data input of which receives a signal at the frequency of a voltage-controlled oscillator (VCO) 1 having a relatively high predetermined operating frequency range (HF). The clock input of the flip-flop is intended to be controlled at a relatively low frequency (BF) with respect to the frequency of oscillator 1. Oscillator 1 is controlled at an intermediary frequency (MF) or by noise. In the example of Fig. 2, a ring oscillator 5 at an intermediary frequency controlling oscillator 1 has been illustrated.

Optionally and conventionally, the output signal of oscillator 1 can be shaped by a comparator 2 having a first input (for example, non-inverting) receiving the output of oscillator 1 while a second input (for example, inverting) receives a reference voltage Vref provided, for example, by a resistive dividing bridge R1, R2 associated with a charging capacitor C. The function of comparator 2 is, with reference voltage Vref, to set a level for the taking into account of the triangular signal provided by oscillator 1 to restore a square signal.

In the example shown, oscillator 5 is formed of three inverters 51, 52, 53 in series. A capacitor C5 conditioning the oscillating frequency connects the output of inverter 53 to ground, generally with an interposed resistor R5 to obtain a triangular signal. The output of inverter 53 (here, after crossing resistor R5) is

looped back on the input of inverter 51 and forms the voltage control signal of oscillator 1. The operation of such a ring oscillator is perfectly conventional and the number of inverters is any number provided that it remains even. Similarly, low-frequency oscillator 4 is formed of inverters 41, 42, and 43 in series and of a capacitor C4 connecting the output of inverter 41 to ground. It thus exhibits the same ring structure as oscillator 5, with the difference that it comprises no resistor. The oscillating frequency is conditioned by the value of capacitor C4.

According to an embodiment of the present invention, clock input CLK of flip-flop 3 does not directly receive this signal provided by low-frequency oscillator 4 but this signal previously crosses a delay element 6. The delay introduced by element 6 is chosen to be at least equal to the maximum period of the signal provided by high-frequency oscillator 1. Ideally, the delay will be equal to this maximum period.

In the example shown, delay element 6 is formed of a series association of several inverters 61, 62, 63, 64, the number of which is chosen according to the significance of the desired delay.

Delay element 6 enables that, even if, incidentally, a period of the signal provided by oscillator 4 appears to be synchronized with the high-frequency signal provided by oscillator 1, the next periods will become desynchronized due to the introduced delay. The equiprobable character of the obtained numbers conditioned only by source 5 of medium frequency or of intermediary frequency thus appears again.

Now, the possible noise introduced by intermediary-frequency oscillator 5 on the power supply necessarily has a frequency smaller than or equal to that of oscillator 1. Indeed, provided that the noise of oscillator 5 has an amplitude smaller than or equal to that of oscillator 1, the latter will mask the possible noise of oscillator 5. Accordingly, this noise at intermediary frequency does not risk causing a synchronization. Accordingly, the oscillator which

conditions the output state of flip-flop 3 effectively is the oscillator of intermediary frequency 5.

This operation is illustrated in Fig. 3 which shows, in the form of timing diagrams, an example of shape of clock signal CLK of flip-flop 3 and of input signal D of this flip-flop.

In the left-hand portion of Fig. 3, it is assumed that the signal of input D is at the maximum frequency of oscillator 1 (minimum period). In the right-hand portion of this drawing, a minimum frequency originating from oscillator 1 (maximum period) is assumed. In the example, the case where the maximum frequency corresponds to twice the minimum frequency is considered.

Assuming an incidental synchronization of the output signal of flip-flop 4 (edge in dotted lines t1 on signal CLK) with the D input of the flip-flop, fixed delay D6 introduced by element 6 (Fig. 2) makes the rising edge of clock signal CLK occur at a time t2. It can thus be seen that the D input state taken into account occurs after one period of the signal of maximum frequency which follows the synchronization time. Accordingly, the risk linked to the synchronization disappears since it really occurs. In the right-hand portion of Fig. 3, a synchronization is assumed at a time t'1. Here again, the introduced delay D6 makes the rising edge of signal CLK occur at least shifted by one period with respect to that of the minimum frequency.

The introduced delay D6 is greater than or equal to the maximum period of fast oscillator 1. It is preferably equal to this maximum period.

An advantage of one embodiment of the present invention is that it avoids the consequences of a risk of synchronization of the high frequency and low-frequency oscillators of the random number generator due, for example, to a pollution of the intermediary frequency signal by noise of the high-frequency signal.

Another advantage of one embodiment of the present invention is that its implementation is particularly simple. Indeed, the modification to be brought to a conventional random number generator with a flip-flop and oscillators

is to add a delay element of a predetermined duration in series with the slow oscillator.

Preferably in one example embodiment, the high frequency is at least 100 times greater than the low frequency, and the intermediary frequency is between 5 and 20 times greater than the low frequency. As a specific example of implementation, the respective oscillator frequencies may be of 1 kHz for the low frequency (BF), 10 kHz for the intermediary frequency (MF), and a frequency ranging between 100 kHz and 200 kHz for the high frequency (HF).

Of course, the present invention is likely to have various alterations, modifications, and improvements which will readily occur to those skilled in the art. In particular, the practical implementation of the delay element and of the oscillators is within the abilities of those skilled in the art based on the functional indications given hereabove and on the application. It should be noted that other oscillator forms than ring oscillators with inverters may be used. Further, it should be noted that the accuracy of the delay introduced by element 6 is not critical. For the equiprobability result to be obtained, over the entire variation range of oscillator 1, there is one half of states 1, and one half of states 0.

Such alterations, modifications, and improvements are intended to be part of this disclosure, and are intended to be within the spirit and the scope of the present invention. Accordingly, the foregoing description is by way of example only and is not intended to be limiting. The present invention is limited only as defined in the following claims and the equivalents thereto.

All of the above U.S. patents, U.S. patent application publications, U.S. patent applications, foreign patents, foreign patent applications and non-patent publications referred to in this specification and/or listed in the Application Data Sheet, are incorporated herein by reference, in their entirety.